TWIC Smart Card Reader Specification
DRAFT v 0.6

Table of Contents

Scope

This document specifies the requirements for smart card readers supporting the Transportation Worker Identification Credential (TWIC). TWIC objectives state the intent to use the credential to access secure areas and information in transportation facilities according to a facility's security plan control requirements. This specification enables varying levels of control in support of threat level risk mitigation plans.

This specification has been developed in concert with the US Department of Homeland Security (DHS) Transportation Security Administration (TSA) Transportation Worker Identification Credential (TWIC) Program.

The mission of the TWIC program is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation's transportation system and their associated information systems. In its development, the TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document.

References

[1] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)

[2] Security Policy for DAL C3 Applet Suite, Dreifus Associates, Ltd.

[3] NISTIR 6887, Government Smart Card Interoperability Specification (GSC-IS) Version 2.1

[4] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers

[5] ANSI/INCITS 377-2004, Information Technology – Finger Pattern-Based Format for Data Interchange

[6] ANSI/INCITS 378-2004, Information Technology – Finger Minutiae Format for Data Interchange

[7] ANSI/INCITS 379-2004, Information Technology – Iris Image Interchange Format

[8] ANSI/INCITS 358-2002, Information Technology – BioAPI Specification

[9] ANSI/INCITS 385-2004, Information Technology – Face Recognition Format for Data Interchange

[10] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)

[11] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts

[12] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[13] SIA AC-01 (1996.10), Access Control – Weigand Card Reader Interface Standard

[14] FIPS 186-2, Digital Signature Standard

[15] FIPS 197, Advanced Encryption Standard

[16] FIPS 46-2, Data Encryption Standard

[17] FIPS 140-2, Security Requirements for Cryptographic Modules

[18] ICAO 9303 Machine Readable Travel Documents

[19] Global Platform Messaging Specification, Version 1.0, Nov. 2003 (Provides a definition of all the roles and responsibilities for all the actors (systems) in a multi application smart card infrastructure and defines reference standard on information exchange (message) between actors)

Control Objectives

Implementation of the Transportation Worker Identification Credential (TWIC) requires the ability to enable local facilities to manage gates/doors according to Local Facility Security Plans, enable local facilities to manage local access according to Network Security Plans, and enable remote verification of a valid and authentic TWIC as well as a valid TWIC card holder. These security plans provide managed control options according to threat level while the TWIC provides part of the means to meet those requirements. These security plans are comprised of two major requirements groupings:

- **Access control requirements:**
  - Door/gate control using biometric and cryptographic functions
  - Door/gate control requiring cryptographic verification of token, no biometrics
  - Door/gate control requiring the token number only
  - Random area personnel checks requiring wireless enabled mobile handheld card reader units incorporating biometric and cryptographic functions
  - Computer/network control incorporating biometric and cryptographic functions
  - Computer/network control incorporating cryptographic verification of token, no biometrics
  - Computer/network control using the token number only
- **Threat/risk control requirements:** the ability for the system to set requirements based on Department of Homeland Security threat level, such as incorporating higher levels of checking and controls at higher levels of threat.

To achieve the control objectives, there must be design features incorporated into the card reader and the relying operational system that profiles and manages the various levels of functions required for reader operation. This can be as simple as releasing a lock on a signal from a local controller upon reading a valid credential number, to a full cryptographically verified and biometrically validated solution involving both the reader and the server.

Options for graduated criteria are defined that state current intentions for operations and how the Transportation Security Administration (TSA) seeks to control those options. These options may be controlled through central control services (e.g., state wide threat level change) and/or local control services at a facility (local facilities assessment of door/gate being protected changes).

The TWIC credential facilitates these control objectives. TWIC supports the range of functions from initial registration into the local facility's Physical Access Control System, through operational use involving the credential number, cardholder biometrics and integrity verification through public key technologies.

The following sections will provide general information about the TWIC credential, its data model, security capabilities and operational use capabilities. Subsequent sections provide detailed guidance on card reader and TWIC interaction and how the TWIC credential supports those requirements. These sections enable reader manufacturers to understand and develop solutions that meet access control requirements using the TWIC credential.

TWIC Capabilities

Card Validation

There are three methods of Card Validation for a TWIC. The first method is via visual inspection that examines the authenticity of the card based on the security features incorporated in the topology. The second method of Card Validation can be performed by a door reader. The reader issues and verifies a challenge/response using a key on the TWIC. The third method of Card Validation requires verification that the card has not been revoked. This verification can be done with a revocation list (PCRL) or through a real-time status transaction with the issuer.

Credential Validation

There are four methods of Credential Validation for a TWIC. The first method is for the door reader to extract a Card Holder Unique IDentification number (CHUID) from the TWIC to verify that it is a valid CHUID. The second method is to extract the issuer signature object and verify the signature covering the CHUID. The third method is the door reader verifies that the CHUID expiration date has not been reached. The fourth method is to verify the CHUID has not expired via a periodic review by the PACS head end or via a real-time status transaction to the issuer.

Cardholder Validation

There are four methods of Cardholder Validation for a TWIC. The first method is to validate the cardholder based on the information printed on the card (photograph, name, etc.) The second method is by requiring the input of a correct PIN and having the door reader issue and verify a challenge/response using a key on the TWIC. The third method is by having the door reader scan a biometric and verify a biometric match of the cardholder to a reference biometric. The reference biometric can be stored on the TWIC or retrieved from a backend system via an index number (CHUID). The fourth method is to verify that the card has not been revoked. This verification can be done with a revocation list (PCRL) or through a real-time status transaction with the issuer.

Data Model Architecture

Each TWIC credential is a hybrid card containing a contactless chip and a contact chip. The TWIC program uses TWIC credentials containing the v2.08 data model. TWIC plans to migrate towards a dual interface technology platform. This will represent a Version 3.xx of the TWIC credential.

All TWIC credentials support the following core elements:

- Card information (issuer, expiration, etc.)
- General information (name of individual)
- Card Holder Unique ID credential number (Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS) version 2.2 compliant)
- Reference biometrics (binding the individual to the credential)
- Security Object containing the Issuer's digital signature for the Identity Assertion

These are the core elements that will be found on both the contact and contactless chips with minor variations depending on version and options supported by the data model. They provide the basis for operational use of the TWIC credential to meet a local facility's graduated security requirements.

The following sections provide specific details on integrity and layout of the TWIC data model.

Credential Numbering

Current physical access solutions focus on a single enterprise. TWIC is designed to enable unescorted access to secure areas of the nation's transportation system. As such, it is designed to enable access across multiple enterprises' physical access control solutions. This highlights the need for an extended numbering schema that is backward compatible with existing solutions, yet allows for a migration to support a very large population envisioned for TWIC.

The TIG SCEPACS, defines the Physical Access Control System data stored on the TWIC. The following are key sections of that document:

- Section 2.1 – defines the Card Holder Unique ID (CHUID)
  - The CHUID contains one mandatory field (FASC-N) and several optional fields
  - The Global Unique ID is defined as an optional field within the CHUID
- Section 6 – defines the Federal Agency Smart Credential Number (FASC-N) (25 bytes)

Figure 1 - Credential Numbering Schema shows the layout of the credential numbering scheme found within the CHUID container of all TWIC credentials. The TWIC program has elected, per the TIG SCEPACS v2.2 specification, to define the credential number as the concatenation of the "System Code || Credential Number" to provide for a number space of 10 billion credentials. The TWIC program has further elected to set the Person Identifier (PI) field of the FASC-N to be the same value as this credential number (each are 10 Binary Coded Decimal digit fields). Every time an individual receives a new TWIC credential, they will receive a new credential number and new PI number in the FASC-N.

The TWIC program has elected to support the optional 16 byte Global User Identifier (GUID) field of the CHUID. The GUID is set such that the low order eight bytes equal the credential number. The high order eight bytes are set to the TWIC issuing Agency Code in accordance with the TIG SCEPACS v2.2 document.

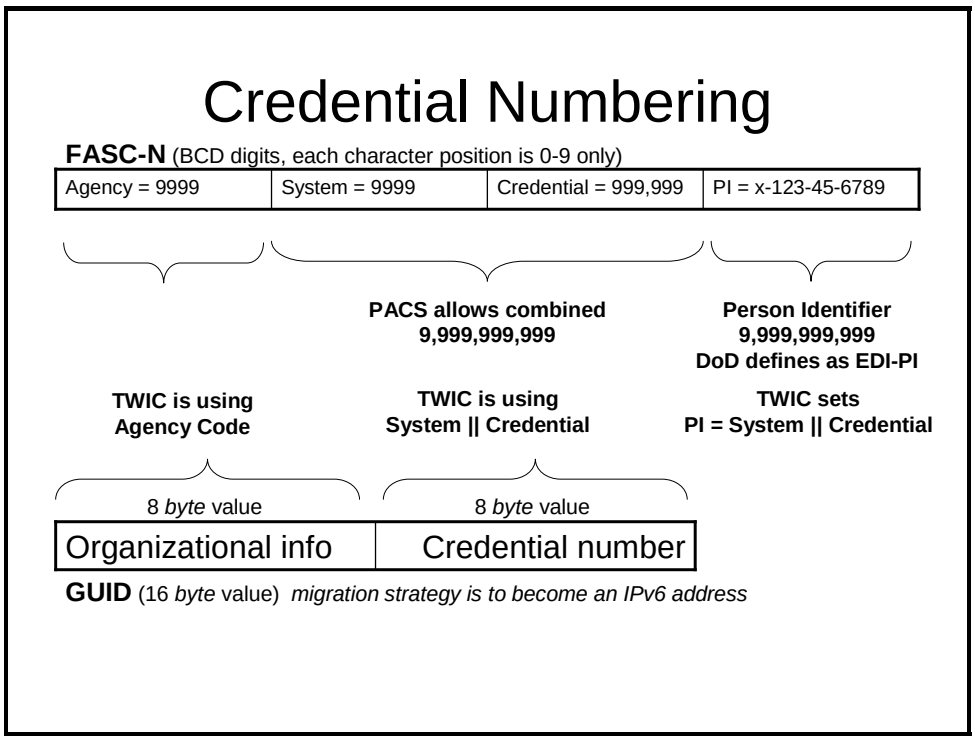

Figure 1 - Credential Numbering Schema

TWIC interface with Smart Card Readers

Each TWIC supports two methods of verifying Physical Access Control Systems (PACS) data stored on the TWIC. The first method uses the FASC-N and is currently the primary means used by existing PACS at Federal Government administered facilities. The second method uses the 16 byte GUID of the CHUID. It is expected that all smart card readers shall transition from the FASC-N to the GUID when interfacing with a TWIC.

The FASC-N is comprised of the following elements:

- Agency Code
- System Code
- Credential Number
- Credential Series (CS)
- Individual Credential Issue (ICI)
- Person Identifier (PI)
- Organizational Category (OC)
- Organizational Identifier (OI)
- Person/Organization Association Category (POA)

Currently to obtain the organization affiliation of a credential the following elements of the FASC-N are used:

- Agency Code
- Organizational Category
- System Code

Generally the Agency Code and the Organizational Category are used during enrollment of an individual at a facility. The Agency Code and System Code are used operationally for physical access at a door reader.

Currently to obtain information regarding the rightful bearer of a credential the following elements of the FASC-N are used:

- Person Identifier
- Organizational Category
- Person/Organization Association Category (POA)

Currently to obtain information regarding the credential number on a smart card the following elements of the FASC-N are used:

Agency Code | System Code | Credential Number | … Credential Series | Individual Credential Issue

The Credential Number does not have an expiration date and is bound to the Individual. If a card is re-issued the Credential Number does not change and a new card is designated by the Credential Series which increases in increments of 1.

The following elements of the GUID are used via smart card readers:

- Prefix
- Subnet ID
- Interface ID

Security Object

The construction of the TWIC Security Object is consistent across all TWIC chips. This security object is in accordance with ICAO 9303 Machine Readable Travel Documents (reference [17]). Each chip has a unique Security Object that protects the integrity of the information stored on that chip as written by the issuer. *Note:* each TWIC credential contains both a contact and contactless chip, so each credential has two unique security objects that are *not* simple copies of the other.

The TWIC Security Object enables the reader to verify the integrity of the information stored on the card by the Issuer. It provides the critical chain of trust link between the relying party and the issuer. All containers of information defined to be within the Issuer Identity Assertion are supported. The security object contains three pieces of information

- The issuer's public key ID information
- A table of hash codes for each container listed in the Issuer Identity Assertion
- The digital signature of the issuer covering the hash table

To verify the integrity of any particular container's information read off of the card, the relying party uses the following steps:

1. Read the container's information
2. Generates a hash of the contents of that container
3. Read the Security Object container
4. Look up the hash in the security object hash table for the container of interest
5. Compare the hash with the hash table entry. If the hashes match, the relying party knows that that the information read from the container is properly constructed.
6. Acquire the correct issuer public key according to the issuer key ID information in the Security Object.
7. Verify the signature for the full hash table as stored in the security object using the issuer's public key. If this signature verifies, then the relying party is assured that the information read is exactly what the issuer placed on the card.

This procedure provides exceptional efficiency, enabling the relying party to only read necessary information, not incurring the overhead required to read the entire Issuer Identity Assertion in order to verify the integrity of a specific container.

Access Control Rules

The access control rules specified here are consistent across all data models for the TWIC. The specifics of the data models are provided in Attachments. These attachments show the specific Application IDs (AID), container IDs, file IDs, tagging structures and access control rules for each data model. At a high level, the following discussion describes the basic guidance on how data is protected on the TWIC.

The following policies are enforced for the contact chip:

- All information stored for the Issuer Identity Assertion is free read.
- PKI services require a PIN to activate the card to use the private key (e.g., generate digital signature).
- The PKI certificates are free read.
- The Issuer Identity Assertion can not be updated except by the issuer using the Global Platform Secure Channel protocols.
- Where supported, extension objects in the TWIC data model must be set up and instanced by the Issuer, using Global Platform Secure Channel [18] protocols. Once instanced, the objects are available according to access control rules set by the issuer (e.g., PIN access) for that object. These objects are not required to be read only.

The following policies are enforced for the contactless chip:

- All information stored in the Issuer Identity Assertion, except for the biometric templates, is free read. (see the following section for contactless access to biometric templates)
- All information written on the contact chip is locked and essentially read only post issuance.

Contactless Access to Fingerprint Biometric Templates

Reading the fingerprint biometric templates from the contactless chip requires a symmetric challenge response protocol using the DESFire's Key0 slot containing the Unique Contactless Diversified Key (CKDC) value defined in *Table 1 - Contactless Key Schema*. This key is used in a challenge response protocol. Each contactless chip has a unique key based on the following diversified key scheme:

Table 1 - Contactless Key Schema

CKMC	Contactless Master key (TSA controlled)
CKDC	Unique Contactless Diversified Key (for each card)
Diversification Data (16 bytes)	7 bytes (UID data)| Padding 7 bytes ('FF FF FF FF FF FF FF')| 2 bytes ('F0 01')
Diversification Method	CKDC = 3DES-ECB (CKMC, 16 bytes diversification data described above)

The basic flow for the native DESFire Authenticate command for the challenge response protocol is:

1. ATR returns the UID for the chip
2. Terminal generates CKDC based on UID and CKMC
3. Select key number setting “Key0” application level key (not the transport key)
4. Perform the DESFire Authenticate protocol
5. If yes, then read binary (biometric template)

Access to the CKMC is under the explicit control of TSA. It will be provided in accord with an explicit agreement with regard to the installation of the reader requiring access to the keying material for contactless biometric access. This SOP will be available in the future from the TWIC Program Management Office.

Data Model Version 2.08

The contact chip for the version 2.08 FOC of TWIC is a GSC-IS version 2.1 compliant JavaCard with 64K EEPROM. This chip uses the Dreifus Applets for GSC-IS services. *Figure 2 - v2.08 Contact* shows the conceptual layout of information in this chip. The extension object directory is used to provide rapid indexing to additional containers and the biometrics on the chip.

The contact chip supports the full Issuer Identity Assertion and two PKI containers for Signature and Email Encryption. Access to all Issuer Identity Assertion containers is free read. Access to the PKI containers requires PIN authentication.

The biometrics stored in this data model are ANSI standards compliant. There are four reference biometrics defined: Facial Image (ANSI 385) , Fingerprint Pattern (ANSI 377), Fingerprint Minutiae (ANSI 378), and if available at enrollment, Iris Polar Coordinates (ANSI 379).

The facial image is provided as an additional operational biometric check, should fingers or iris not be available. The facial image can also be used in human verification operations when examining the credential to match the bearer. Iris is offered as an optional feature of the data model and is for testing purposes of TWIC. Iris is not used operationally by the TWIC program at this time.

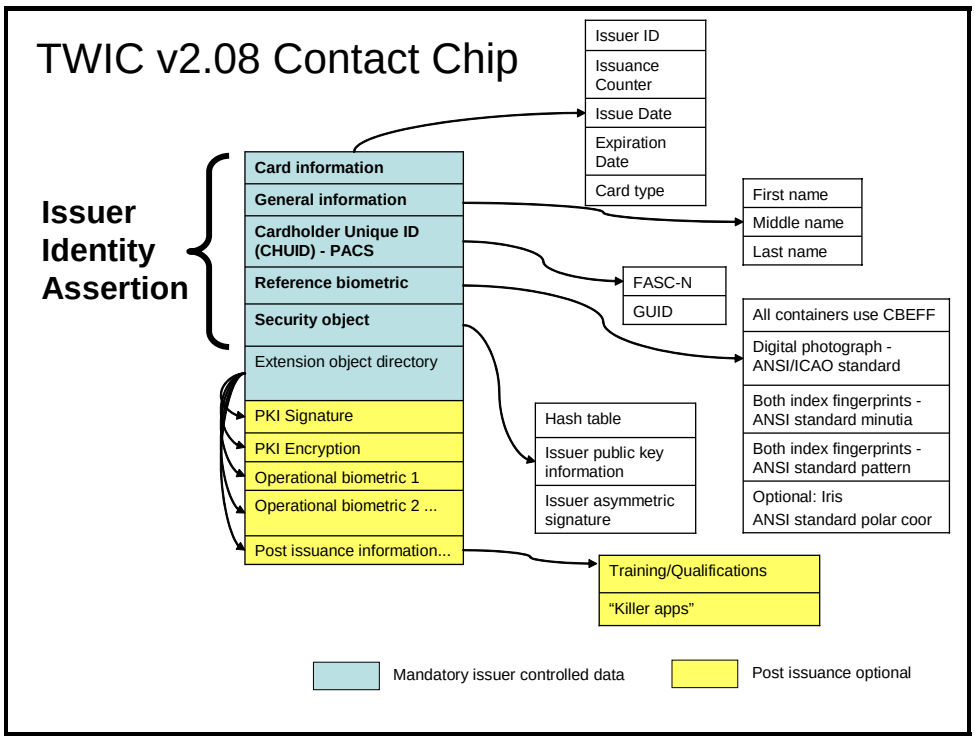

Figure 2 - v2.08 Contact

The contactless chip for the version 2.08 FOC of TWIC is a DESFire card with 4K EEPROM from Philips. *Figure 3 - v2.08 Contactless* shows the conceptual layout of information in this chip.

The contactless chip supports the full Issuer Identity Assertion. Access to all Issuer Identity Assertion containers, except for the biometric container, is free read. Access to the biometric container requires a symmetric key challenge response protocol using the DESFire's Key0. PIN is not supported on the contactless chip.

Information in this data model has been optimized to enable storage of both Pattern and Minutiae based templates. This enables enhanced operational efficiency and use of either matching technology, depending on biometric equipment and software deployed by a facility.

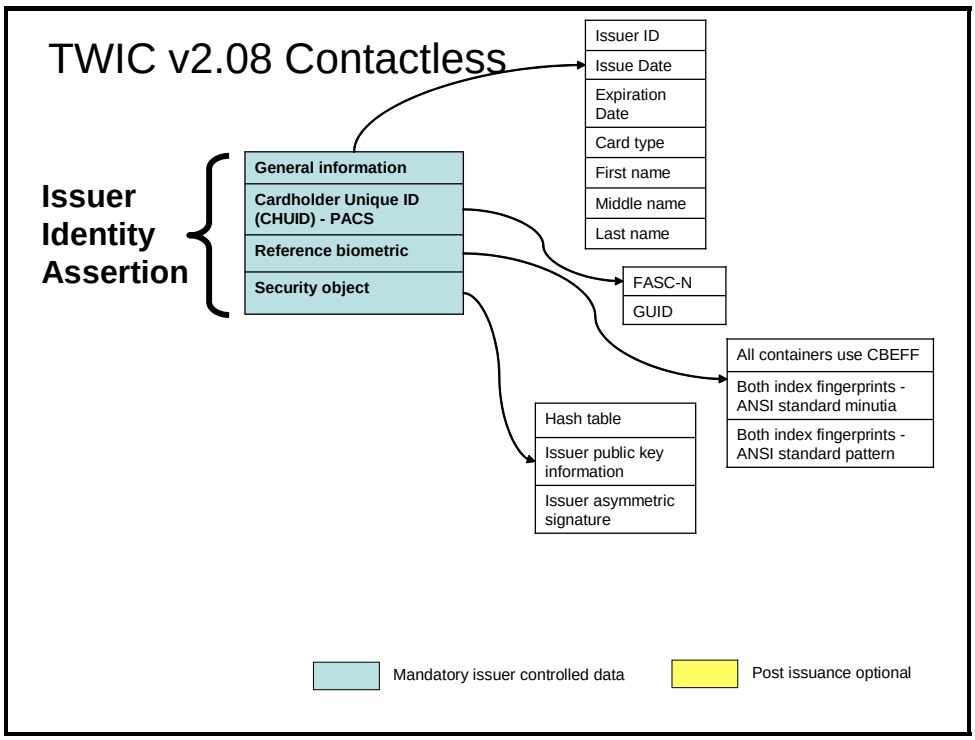

Figure 3 - v2.08 Contactless

Graduated Criteria Capabilities

The TWIC credential supports a set of graduated criteria for authentication of the credential itself, and the bearer of that credential at the time of challenge. Establishing a chain of trust is a result of performing both a Credential Authentication and Cardholder Authentication.

Table 2 - Credential Authentication shows the options available to prove that the credential is authentic. These features work for both the Contact and the Contactless chips. CA4 is only available on the contactless chip with respect to access of the biometric at this time. There may be future methodologies offered that include a digital signature generated by the Credential that is subsequently verified by the Reader. CA5 and CA6 involve direct checking of the TWIC Hotlist Services.

Table 2 - Credential Authentication

Level	Criteria	Description
CA0	Visual Inspection	Verify human readable security graphical features
CA1	Data Present	Unsigned data is found on a credential
CA2	Signed Data	Issuer-signed data is found on credential, no cryptographic checking is performed
CA3	CA2 + Signature Verify	Issuer-signed data is found on the credential and verified
CA4	CA3 + Challenge	Above + credential demonstrates it knows the authentication secret (i.e. perform mutual authentication with the CKDC)
CA5	CA4 + Revocation Check	Above + Reader checks most recent revocation list from issuer to verify credential has not been revoked
CA6	CA5 + Issuer Check	Above + Reader performs a real time check with issuer service to verify that credential is still valid

Table 3 - Cardholder Authentication shows the options available to demonstrate that the credential is in the possession of the rightful cardholder.

Table 3 - Cardholder Authentication

Level	Criteria	Description
CH1	Possession	Cardholder is in possession of the credential (photo ID)
CH2	CH1 + PIN	The cardholder has entered the correct PIN
CH3	CH1 + Bio	The cardholder has passed a biometric match
CH4	CH1 + PIN + Bio	The card holder has entered the correct PIN and passed a biometric match.
Note: This scheme applies whether the authentication is performed by the credential or by an external entity (reader, PC, door controller…) *The guiding principle is that the authenticating entity must perform the match.* Thus: • Credential-based: The card must perform the PIN validation and/or biometric match. • External Auth: External entity must perform the PIN validation and/or biometric match.		

It is recommended that these tables be used in concert for relying parties to establish appropriate security levels of trust for any given transaction. The following are given as guidance and options available to local facilities for access control decisions:

- Initial registration of an individual to a local PACS should consider minimum of CA5 and CH3. This provides assurance that the credential is still valid according to its issuer and that the rightful bearer is present. Once confirmed, privilege can be granted to that individual using that particular credential.
- When an individual requests access at a low risk control point, a local PACS should consider a minimum of CA2. It is strongly recommended that CA3 be the minimum, as this provides minimum assurance that the credential has not been tampered.
- When an individual requests access to a medium risk control point, a local PACS should consider a minimum of CA3 and either CH2 or CH3, confirming an unaltered credential and the presence of the legitimate bearer.
- When an individual requests access to a high risk control point, a local PACS should consider a minimum of CA5 and CH4, confirming an unaltered credential that is still in good standing with the issuer, and the presence of the legitimate bearer through three factor authentication.

Local facilities should periodically check the integrity of TWIC credentials registered to their system by confirming that credentials have not been revoked on the TWIC Hotlist.

Reader Security and Data Requirements

The reader shall implement the processing of the CHUID per the requirements of the TIG-SEPACS guidance (see reference [1]) for both the low and medium protection profiles.

The reader shall be field configurable to allow selection of CHUID data elements for inclusion in the Wiegand data output stream, including parity, bit position and data length. The GUID is the authoritative credential number that guarantees uniqueness of credentials throughout the TWIC program and should be used in favor of the FASC-N.

For medium assurance profile operation, the reader configuration utility shall support the configuration of the credential authentication parameters as required by the TIG-SCEPACS guidance.

Security keys are required to read the biometric containers over the ISO 14443A/B interface. These keys must be user customizable using a manufacturer-supplied configuration utility. The reader shall support ISO 7816 compliant authentication methods to provide mutual authentication between credential and reader. The credential media is digitally signed by the issuer. The reader should be able to verify this signature. Authentication and signature methods shall use algorithms that are compliant appropriate government standards as specified by FIPS 186-2, FIPS 46-2 and FIPS 197.

The reader shall be designed such that memory used for storage of security keys is protected from all forms of attack on the memory device itself that would result in disclosure of the security keys for the reader and associated media. The manufacturer shall design for compliance to FIPS 140-2 level 3 requirements or a National Information Assurance Partnership (NIAP) certification for Common Criteria at an EAL 4+ to demonstrate this level of protection.

The manufacturer shall provide a configuration utility, key management utility and any other configuration software required free of charge in CD format or by download from the manufacturer's web site.

TWIC Modes of Operation

There are 4 environments in which a TWIC interfaces with a reader:

- Enrollment
- Physical Access Control Systems
- Logical Access
- Wireless Remote Verification

Enrollment

The TWIC is presented to an Enrollment Station at a facility where it is read via a contact interface. At this time the credential and personal information is acquired into the system. Depending on particular system requirements, a PIN and/or biometric check may be required at this time. The biometric check may be match-to-card or match-to-system. All required information is read from the card at this time and stored according to the security policies of the local facility.

Physical Access Control Systems (PACS)

Generally a TWIC will be used at a door or gate that may or may not be manned. The interface between the TWIC and reader may be via the contact or contactless interface according to particular system specification. There may also be a requirement that a PIN and biometric check be completed successfully at the reader to gain access.

Logical Access

A TWIC may be used to gain access to a network or a personal computer. The interface between a TWIC and the reader will be via the contact interface only. There may also be a requirement that a PIN and biometric check be completed successfully to gain access. Additional computer security policy requirements may have to be met.

Wireless Remote Verification

A TWIC can be interrogated and verified remotely via wireless enabled mobile handheld units. The interface between the TWIC and reader may be via the contact or contactless interface. There may also be a requirement that a PIN and biometric check be completed successfully for verification of the credential and the card holder. The mobile handheld units will be operated by designated, authorized personnel.

Electrical and Physical Requirements

Beyond these control objectives are electrical and physical interoperability requirements. These are objectives that state the nature of the environment and technologies in place that the reader must interoperate with to be compliant and successful.

The purpose of the door reader unit is to provide the physical interface between the TWIC credential and the physical access control system controlling access to that portal (turnstile, door, gate, ramp, etc.).

General Requirements – hard mounted readers

The reader shall provide for single- or dual-gang mounting for non-metal or metal wall mounting, non-metal or metal vehicle stanchions and non-metal or metal pedestals. Mountings shall be tamper-proof.

The reader shall be sealed to a rating of IP65. For card only or card + pin pad readers, the protection rating is required for the reader itself. For biometrically enabled devices, the reader components may be offered in an enclosing cabinet that achieves the rating required.

The reader shall operate on 8-25 VDC. Current requirements shall not exceed 1.5 Amps.

The reader shall operate within a temperature range of 20-120F degrees.

The reader shall operate in a humidity range of 5-90%, non-condensing.

The reader shall be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources.

The reader shall be FCC and CE certified, and shall conform to the ISO14443A/B.

The reader may support an ISO 7816 compliant contact interface as a manufacturer's option.

The reader may contain an encrypted numeric keypad to enable secure PIN entry per Seaport PACS requirements.

The reader shall have an approximate read range of 10cm when used with the contactless card media.

The reader shall require that a card, once read, must be removed from the RF field for one second before it will be read again to prevent multiple reads from a single card presentation.

The reader shall be capable of reading the access control data from the card, performing the necessary authentication steps, and transmitting the credential data as require by the Seaport PACS.

The reader shall enable communications ports as required by the Seaport PACS cable plant and control panels. Minimum options required are:

1. Wiegand port for connection to standard access control panels.
2. RS-485 or 10/100baseT for connection to computer systems or access control systems.

The reader shall support a minimum of two operational modes:

1. Internal control – All required processing is implemented in the reader and Wiegand data is transmitted to the access control system.
2. Host control - Externally controlled processing for applications including online credential authentication and biometric template retrieval.

The reader shall provide visual and audio indicators with regard to access grant, deny, reason codes, requests for re-read of biometric, etc.

For biometrically enabled readers, the biometric device should be embedded in the same chassis as the reader. If a separate biometric device is used, the wiring between the reader and biometric unit must not be exposed.

The reader shall utilize flash memory to allow for future enhancements to be added in the field.

General Requirements – mobile handheld reader

Offeror shall provide options enabling mobile interrogation and verification of the credential. Options shall support direct access to the Seaport Access Control System via secure wireless interface.

This device is envisioned to be used in a minimum of two operational modes:

- At a gate control location to interrogate credentials within a vehicle with multiple occupants
- Authorized security personnel performing random challenge throughout the facility

General Requirements – contact reader

- API: PC/SC compliant with corresponding drivers for MS Windows
- Option for other systems: MAC OS Systems, Linux, Win CE, etc.
- Ability to support faster communication speed
  - Support of the PPS Protocol
  - Indicate the values of the TA1 byte supported by the reader (combination of I/O speed and frequency)
- Amount of power available for card inserted into the reader
- Host connection type (USB or other)
- Contact insertion cycles guaranteed for at least 50,000
- Shall be protected against short circuits
- Shall support T=0 and T=1 protocols
- Support of all APDUs defined in ISO 7816
- Certifications: WHQL, EMV Level 1, USB (if applies) FCC
- Operating voltages, temperature, etc.
- Options:
  - Firmware upgradeable in the field
  - Support cards with different VCC (ISO 7816 Class A required, B & C Optional)

General Requirements – contactless reader (PC-based)

- Shall support ISO 14443 parts 1, 2, 3, and 4 (T=CL protocol)
- Type A and B support required
  - API:
    - PC/SC compliant with the corresponding drivers for windows
    - Option for MAC systems

    - Anti-collision as per ISO 14443 is not a requirement as long as the reader detects multi card presentations
- Options to indicate:
    - Ability to support faster communication speed (424 Kbps or higher)
    - Auto RF-field tuning

Performance Requirements

The card reader shall support data interrogation within one-half (0.5) second, enabling the find, read, and decode of stored and/or encoded card information within one (1) second after the credential is interrogated.

The card reader shall be capable of 99.99% data read accuracy.

The card reader must accurately interrogate the credential 99.99% of the time on the first attempt. When reference or operational biometric data is read, the reader shall support biometric verification within two seconds of credential interrogation.

Biometric matching shall have a verification (1:1) accuracy of 99% or higher. The biometric Equal Error Rate (EER) shall not be more than 1% for verification.

Fingerprint biometric technology shall be capable of template creation from a single image capture.

Fingerprint reader image resolution shall be 500dpi or higher.

Biometric matching performance shall address the high potential for operational requirements in unclean working environments and with users having worn fingerprint ridges and artifacts.

Biometric devices shall offer liveness[1] detection as a manufacturer's option.

When a reference or operational biometric verification (1:1) is initiated, the correct result (accept or decline) shall be accomplished on the first attempt at least 90% of the time.

Biometric processes and performance is further described in ANSI/INCITS 383.

1 Liveness may include subdermal, vein, capacitive or other techniques.

Quality and Reliability

Readers shall have a mean time between failures (MTBF) of 10,000 hours or greater.

Readers shall not require mean time between maintenance (MTBM) of less than six months.

Delivery

The reader shall include technical manuals covering installation, operation and maintenance of the units.

Units will be packaged suitable for shipment to installation points.